ATTACHMENT 17

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SURGICAL INSTRUMENT SERVICE COMPANY, INC.,

Plaintiff(s),

v.

INTUITIVE SURGICAL, INC.,

Defendant(s).

Case No. 3:21-cv-03496-VC

Honorable Vince Chhabria

REBUTTAL EXPERT REPORT OF KURT HUMPHREY

Complaint Filed: May 10, 2021

Highly Confidential – Subject to Protective Order

TABLE OF CONTENTS

I. INTRODUCTION

1. I am an expert in reverse engineering (RE) industrial and consumer microelectronic devices, components and systems including RFID products such as smart EMV smartcards and other proximity integrated circuit cards (PICCs). Over the course of my career, I have reverse engineered a large number and wide variety of semiconductor devices including microprocessors and non-volatile memories such as EEPROMs and Flash products for OEMs such as Apple, Alcatel-Lucent (Nokia) and others. I currently work as a Managing Director and Principal Technologist at IP Enginuity LLC. I have held that position for 17 years. The knowledge and experience obtained during my 20+ year history in integrated circuit (IC) device and smart sensor processing provide me with the expertise necessary to offer expert opinions in this case.

2. I am submitting this rebuttal report at the request of Haley Guiliano LLP, counsel for Surgical Instrument Service Company, Inc. ("SIS"), the named plaintiff in the lawsuit captioned on this report's first page. I am being compensated for my time spent in preparing this report at an hourly rate of $450/hr. If asked to testify in this lawsuit, I will be compensated at the rate of $450/hr for deposition testimony and $450/hr for testifying at trial. My compensation does not depend in any way on the outcome of this action.

3. On December 2, 2022, I submitted an opening expert report in this litigation opining on certain issues relating to the encryption utilized on Intuitive Surgical Inc. ("Intuitive") X and Xi EndoWrist products.

4. My qualifications, including a summary of my career, a list of my professional publications and presentations, my curriculum vitae, and description of my current position are described in my Opening Report and exhibits to that report.[1]

[1] Expert Report of Kurt Humphrey, *Surgical Instrument Service Company, Inc. v. Intuitive Surgical, Inc.*, Case No. 3:21-cv-03496-VC, December 2, 2022 (herein after "Opening Report").

5. I have been asked by counsel for SIS to review, analyze, and respond to the expert report submitted on behalf of Intuitive Surgical by Paul D., Martin, Ph.D.[2]

6. The purpose of this rebuttal is not to retread ground that I covered in my Opening Report or to respond and rebut every error and flaw in the Martin Report. The lack of response to any particular claim or argument does not mean that I agree with it. Nor is the purpose of this Rebuttal Report to detail each misstatement of fact in the Martin Report. In summary, however, nothing presented in the Martin Report changes the opinions I have expressed in this matter.

7. A list of materials that I considered in forming my opinions in this Rebuttal report is attached as Appendix A.

8. In examining the Martin Report, I note that although new materials are cited, I consider them to be cumulative of materials I have previously considered when preparing my Opening Report.

9. On the basis of my review of the Martin Report and materials considered in the Martin Report, I stand by the analysis in my Opening Report, the opinions thereon, and nothing causes me to change the analysis of that initial report.

II. SUMMARY OF OPINIONS

10. Dr. Martin's discussion of "additional security concerns" for wireless communications in fact demonstrates that using RFID was an inferior solution to the proven pogo-pin methodology Intuitive used for the wired Si EndoWrist instruments.

11. Other purported differences between the Dallas and Atmel chips identified by Dr. Martin were not as a factual matter actually used by Intuitive to justify the switch to the wireless Atmel chip and are essentially irrelevant or trivial from an engineering perspective.

[2] Expert Report of Paul D. Martin Ph.D., *Surgical Instrument Service Company, Inc. v. Intuitive Surgical, Inc.*, Case No. 3:21-cv-03496-VC, January 18, 2023 (herein after "Martin Report").

III. DISCUSSION

12. I disagree with Dr. Martin's generalization "that a wireless communication channel offers general improvements over a wired communication channel."[3] There are certainly pros and cons to both wired and wireless communications, however "improvements" associated with one type of communication over the other is often largely a matter of the specific application being considered.

13. Those tradeoffs typically weigh in favor of wireless communications where the specific application requires that the device(s) be untethered, *i.e.*, are typically not physically connected to each other. In the case of EndoWrists and da Vinci surgical robots, and as demonstrated in the S/Si systems, the EndoWrists physically attach to the robot arm in a precise manner, such that there is no need to implement a wireless option for X/Xi EndoWrists (which are likewise physically attached to the robot arm). The physical connection between the EndoWrists and robot arm provides precise engagement to control the EndoWrist rotational disks that in turn control the patient-touching physical movement of the EndoWrist distal end, and in some instruments provides an electrical connection for electrocautery that is used for sealing of patient tissue.

14. In view of these other physical connections that directly impact patient safety, the acceptably low failure rate of the pogo pin electrical connection in Si instruments,[4] [redacted] [5] and direct evidence that Intuitive's design goal was to prevent resetting of the Xi

[3] Martin Report at ¶ 23.
[4] Intuitive-00967510 at Intuitive-00967513; Opening Report at ¶¶ 40-42.
[5] Intuitive-01004232 at Intuitive-01004238-239; Deposition of Shark Somayaji at 132:8-138:2; Opening Report at ¶¶ 56-58.

EndoWrist counter,[6] it seems clear that Intuitive's wireless design choice was primarily motivated to prevent resetting of the EndoWrist usage counter.

15. I also disagree with the unsupported assertion that "wireless technology has a lower manufacturing complexity".[7] On the contrary, wireless devices, and particularly RF devices, require the fabrication of RF-specific components, *e.g.*, integrated antennas, filters, tuning circuits, etc., that are absent in conventional wired integrated circuits. The rather modest processing performance, speed, and memory requirements for both S/Si and X/Xi generations of EndoWrists are easily satisfied using commodity, off-the-shelf chips whether wired or wireless.

16. Moreover, as admitted in Dr. Martin's report, RFID introduces additional risks and problems such as wireless interference, eavesdropping, and a variety of attacks.[8] For example, Dr. Martin concedes that "The threat model with respect to the wired connection is simpler than the threat model with respect to the wireless connection."[9] He also states that "Therefore, for the wireless system, the threat model is a superset of the threat model for the wired system."[10] In sum, the Martin Report makes a strong and detailed case for the advantages of maintaining wired communications between the EndoWrists and the da Vinci robot arm as opposed to dealing with the "security vulnerabilities of wireless systems."[11] Switching from the simpler threat model associated with the wired DS2505 1-Wire® chip (or similar commodity wired solutions) to the more complex threat model associated with the wireless Atmel CryptoRF chip (or similar commodity wireless solutions) in the later X/Xi generation EndoWrists strongly counsels against

[6] Intuitive-02068695-97; Intuitive-02068686; Opening Report at ¶¶ 48-51.
[7] Martin Report at ¶ 23.
[8] Martin Report at ¶¶ 39-45.
[9] Martin Report at ¶ 33.
[10] Martin Report at ¶ 33.
[11] Martin Report at § V.

employing a wireless connection, particularly when the EndoWrists are required to be physically connected to the da Vinci robot arm during surgical use.

17. Dr. Martin suggests that some of the features of the Atmel CryptoRF device disclosed in the device datasheet, *e.g.*, memory size, provide improvements used in the X/Xi systems over the DS2505 chip used in the S/Si systems but offers no evidence to support the notion that it was necessary or important for Intuitive to utilize any of these features.[12] Dr. Martin offers no evidence to suggest that deploying any of the features he identified for the Atmel CryptoRF device gives the X/Xi EndoWrist instruments any competitive advantages over the previous generation S/Si EndoWrist instruments. Proving the absence of any evidence that Intuitive needed any of these features of the Atmel chip, Martin hypothetically speculates that the increased memory size associated with the Atmel CryptoRF device "allows for more data to be stored and transferred either as part of the EndoWrist X/Xi or, if not used in this context allows for easier upgrades in later EndoWrist models that might want to store and transmit more data." (emphasis added). In any event, both wired and wireless chips are commodity components that are available in a variety of configurations for memory size, transmission speeds, and the like. In my opinion, there is nothing compellingly unique about the Atmel CryptoRF device with respect to such features. For instance, the "Dallas" family of 1-Wire® memory offerings extended beyond the legacy DS2505 chip, including products such as the DS28EC20 20Kb 1-Wire EEPROM with 20 times the memory of the DS2505 chip and "200k Write/Erase Cycle Endurance."[13] The DS28EC20 datasheet also lists "Medical Sensors" as one of its primary applications and appears to have been available for design-in at least as early as 2007.[14] Other than the secure wired versus RF wireless communication difference, the key distinguishing feature between the Atmel

[12] Martin Report at ¶ 56(i).
[13] DS28EC20 20kb1-Wire EEPROM Datasheet, p. 1
[14] *Ibid*, p.27

CyrptoRF chip and the "Dallas" chips is the Atmel chip supports encrypted communications and 1-Wire memories do not. Dr. Martin does not cite to any evidence suggesting that Intuitive's switch from the wired communication technology to a wireless connection provides substantially improved capabilities for the EndoWrist instruments in terms of the instrument's reliability, performance and/or functionality when used during a surgical procedure.

18. Dr. Martin draws the unreasonable inference that because the Atmel CryptoRF datasheet includes a reliability metric and an endurance metric that are not similarly disclosed in the DS2505 datasheet that this is somehow indicative of greater reliability and endurance for the Atmel chip.[15] The fact that Dallas Semiconductor (subsequently acquired by Maxim and more recently Analog Devices) chose not to include these specific reliability metrics or address reliability specifically in the DS2505 datasheet does not suggest the DS2505 chip is any more or less reliable than the Atmel chip. On the contrary, the fact that the DS2505 chip is a 20-25 year old product still in commercial production is a testament to its real-world reliability and endurance track record. Indeed, I'm not aware of any design issues or problems reported by Intuitive engineers or customers with respect to the S/Si EndoWrists that were traced to or associated with the use of the DS2505 chip. Likewise, Dr. Martin has not provided any evidence in his report that using the DS2505 chip caused problems or issues with the either the safety, effectiveness, or data security of the S/Si EndoWrist instruments. Nor has Dr. Martin identified any issues with the level of data security provided by the wired system in the S/Si EndoWrists; in fact, the Martin Report supports the proposition that a wired connection offers superior data security.

19. Dr. Martin makes a reference to inclusion of an integrated tuning capacitor in the Atmel chip and lack of an advertised integrated tuning capacitor in the DS2505.[16] Since the

[15] Martin Report at ¶ 56(ii).
[16] Martin Report at ¶ 56(iii).

DS2505 is a conventional wired device and contains no RF or wireless components, an integrated tuning capacitor is unnecessary and irrelevant to this discussion.

20. Dr. Martin also states the Atmel chip offers "nearly twice as fast data access times than the Dallas chip." Actually, the Dallas chip was shown to be slightly faster than the Atmel chip for 1st and 2nd read access times in the referenced table.[17] I would hasten add, however, that data access times for either chip are likely more than adequate for the X/Xi application and that data access times are unlikely to be a significant design factor in choosing one chip over the other for this application.

21. Dr. Martin remarks that "Mr. Humphrey also ignores the benefits of wireless technology versus wired technology entirely in his analysis."[18] The purported benefits of wireless technology cited by Dr. Martin do not readily apply to EndoWrists. The primary benefit of wireless technology is reflected in the terminology, *i.e.*, it is without wires and thus physical connection is not required. The primary objective in wireless communications is to enable information transfer without wires, *i.e.*, in applications where wires are impractical. For example, the smartphone market would be non-existent if smartphones required wires to physically connect to a cell tower. Having worked extensively in automotive, aerospace, and military electronics, I can attest to the fact that the performance and reliability requirements required by the carmakers generally exceed those required for similar military and aerospace components. These stringent demands on automotive electronics are one of the main reasons wireless devices are rarely used in automotive electronics unless physical connections are impossible or impractical, *e.g.*, remote keyless entry (RKE) systems, tire pressure monitoring systems (TPMS) and radio/Bluetooth infotainment applications. The preponderance of automotive electronic devices and sensors,

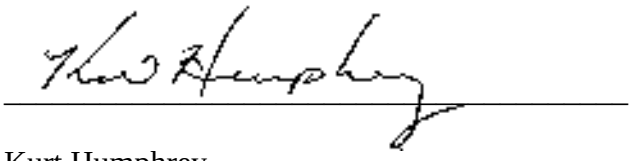
[17] Intuitive-00544903 at 5094.
[18] Martin Report at ¶¶ 57-59.

however, are connected or hard-wired via pins, boards and wiring harnesses. These fundamental justifications for using wireless technology simply do not apply to EndoWrists. Intuitive intentionally designed its EndoWrists to be physically connected to a surgical robot via a specific and repeatable physical interface. Therefore, there is no compelling engineering justification, inherent design need or motivation to use wireless technology in the X/Xi EndoWrist design.

22. In my opinion, there is no compelling engineering reason for the change from a wired to a wireless connection, and corresponding encryption changes, from S/Si EndoWrists to X/Xi EndoWrists. In fact, by Dr. Martin's reasoning these changes left the chip more vulnerable to a malicious attack.[19] The most reasonable explanation is that the change was made to make it more difficult to access the use counter on X/Xi instruments.

IV. CONCLUSION

23. In sum, Dr. Martin's report is devoid of evidence or reasoned argument that Intuitive's X/Xi wireless and encryption design choices were driven by anything other than its expressed desire to block third parties from accessing and modifying the use counter. If anything, his opinions about the significant problems with wireless communications buttress the opinions stated in my Opening Report, since it makes little sense to take on these additional risks when the EndoWrists necessarily physically connect to the robot arms.



Kurt Humphrey

February 13, 2023

[19] Martin Report at ¶¶ 31-37, 40-45, 47, 49.

Appendix A

Materials Considered

- All materials considered in Expert Report of Kurt Humphrey., *Surgical Instrument Service Company, Inc. v. Intuitive Surgical, Inc.,* Case No. 3:21-cv-03496-VC, December 2, 2022

Case Documents

Pleadings

- Complaint, *Surgical Instrument Service Co., Inc. v. Intuitive Surgical, Inc.*, No. 3:21-cv-03496-VC (ECF 1) (May 10, 2021)
- Consolidated Amended Class Action Complaint, *In re: da Vinci Surgical Robot Antitrust Litigation*, Lead Case No. 3:21-cv-03825-VC (ECF 52) (Sept. 9, 2021)

Expert Reports

- Expert Report of Christy Foreman (Jan. 18, 2023)
- Expert Report of Kurt Humphrey (May 10, 2021)
- Expert Report of Kurt Humphrey, submitted in the matter of *Rebotix Repair LLC v. Intuitive Surgical, Inc.*, Case No. 8:20-cv-02274 (M.D. Fla.) and dated July 26, 2021

Deposition Transcripts and Exhibits

- Deposition of Grant Duque 30(b)(6) (November 8, 2022)
- Deposition of Grant Duque (November 8, 2022)
- Deposition of Sharathchandra "Shark" Somayaji (November 4, 2022)
- Deposition of Margaret Nixon (October 7, 2022)

Produced Documents

- Intuitive-00002201 - da Vinci Si Surgical System User Manual
- Intuitive-00002502 - da Vinci Xi System User Manual
- Intuitive-00499468
- Intuitive-00506505
- Intuitive-00538994
- Intuitive-00544903
- Intuitive-00861667
- Intuitive-00994614
- Intuitive-00999731 (Somayaji Deposition, Ex. 224) - Atmel CryptoRF EEPROM Memory Summary Datasheet
- Intuitive-01004232
- Intuitive-01004242
- Intuitive-01004385

Other Documents

- Annalee Newitz, *The RFID Hacking Underground*, WIRED, (May 1, 2006), available at: https://www.wired.com/2006/05/rfid-2/.
- Atmel CryptoRF EEPROM Data Sheet.
- Dale Anderson, *Understanding Crypto Memory the World's Only Secure Serial EEPROM*, ATMEL (2004).
- Dallas Semiconductor DS2505 Data Sheet.
- GITHUB, *Proxmark3*, available at: https://github.com/Proxmark/proxmark3 (last visited Jan. 18, 2023).
- Grassi et. al., *Digital Identity Guidelines*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, June 2017, available at: https://doi.org/10.6028/NIST.SP.800-63-3.
- KASPERSKY, *What is Spoofing - Definition and Explanation*, available at: https://www.kaspersky.com/resource-center/definitions/spoofing (last accessed Jan. 18, 2023).
- Martin et. al., *Applications of Secure Location Sensing in Healthcare*, Proceedings of the 7th ACM International Conference on Bioinformatics, Computational Biology, and Health Informatics (2016).
- OPENSSH, available at: https://www.openssh.com/ (last visited Jan. 18, 2023).
- Products Specifications, INTEL, available at: https://ark.intel.com/content/www/us/en/ark/search/featurefilter.html?productType=873&1_Filter-SocketsSupported=3562 (last visited Jan. 18, 2023).
- RFID Readers, AMAZON, available at https://www.amazon.com/RFID-Readers/s?k=RFID+Readers (last visited Jan. 18, 2023).
- Tyler Petersen, *RFID Card Security and Attacks*, (Oct. 15, 2020), SIKITCH, available at: https://www.sikich.com/insight/rfid-card-security-attacks-and-prevention/#:~:text=An%20MITM%20attack%20against%20an,gain%20access%20to%20the%20building.
- Dallas Semiconductor (Maxim Integrated) DS28EC20 20Kb 1-Wire EEPROM Data Sheet.